制御システムにおけるセキュリティフレームワーク

A study on security framework for operation and control system

李哲・法制倫理分科会・情報セキュリティ大学院大学

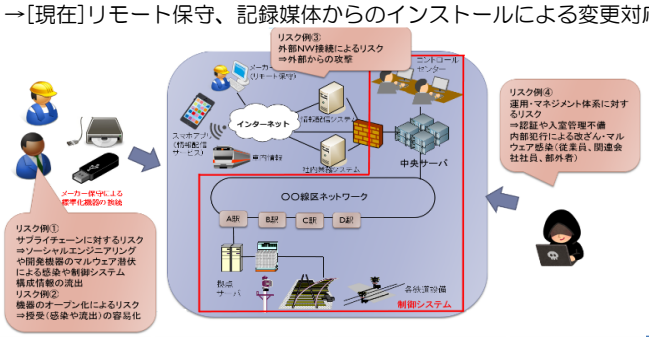
Abstract: For past years, the control system has designed and assure certain level of security quality utilizing unique protocols, a set of hardware and software, and the closed networks. However, after 2000, big changes applied such as interfacing to external networks, implementing systems with open technology and field data utilization both for operations and customer service. In this paper, a new framework is proposed which enables ISMS-based security to the control systems composed by existing unique systems, operations and management system. To confirm proposed framework, the model case study for the railway control system has carried out.

研究目的
制御システムのセキュリティ上の課題を考慮したセキュリティ対策を目的とする。また、ISMSを基準とした管理策でのリスク管理、他システム接続や今後の改修において、セキュリティ実施状況の管理を容易にすることにおいても目的とする。

提案手法
①制御システムOTのセキュリティ例外対象をISO/IEC27002を基準としての明確化
②例外対象一覧の運用方法を提案し、あらゆる現場で運用できるセキュリティフレームワークの提案

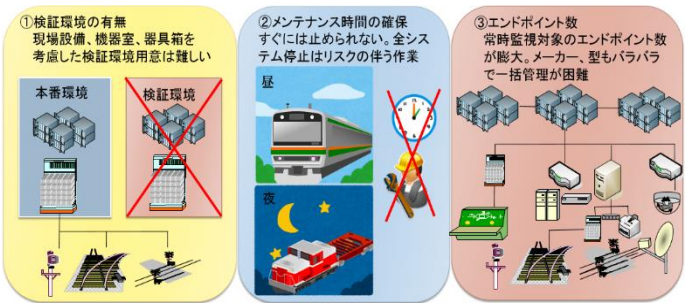
1.制御システム変化から生じる課題

■制御システムの変化を以下に表し、生じるリスク例を図で示す
①[昔]シンプルで電気的機器構成→[現在]複雑で情報、NW機器の導入
②[昔]クローズドネットワーク→[現在]外部NWやシステム接続・連携
③[昔]独自プロトコル・技術→[現在]オープン化機器の採用
④[昔]現地保守、機器交換による変更・改修
→[現在]リモート保守、記録媒体からのインストールによる変更対応



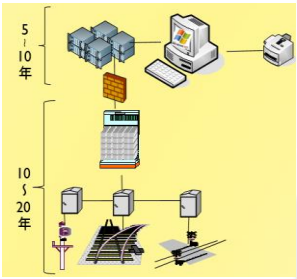
2.セキュリティ面の課題

(1)セキュリティパッチ適用の難しさ
セキュリティパッチ適用には以下の3点の原因がある



(2)制御システムの可用性低下の懸念
安全性＋機密性＋完全性(セキュリティ)と可用性のバランス調整(チューニング)が難しく、可用性を落とさない構成を優先してしまう

(3)ライフサイクルの違い
OT機器とIT機器の更新頻度の違いからIT機器は更新するとしても同型種の旧機器で更新されるだけ(OSもベンダーサポートが終わってもWinXPのまま等)
⇒セキュリティ対策の陳腐化へ

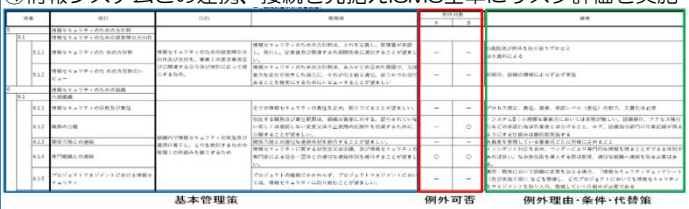


(4)不明確なセキュリティーポリシーによる課題
OTとITの境界が不明確でどちらに主体、責任があるか分からない
⇒現場に主体がないため、実運用では例外の恒常化、形骸化が発生

3.提案手法

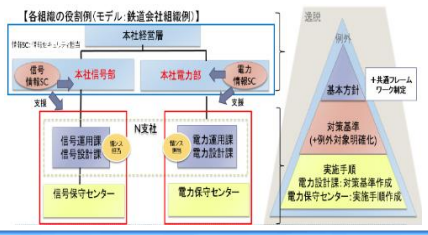
本研究の提案手法として、前述の課題からOT独特の特性を考慮しISMSを拡張してOTのセキュリティガイドラインとするため管理策を検討する。OT観点で管理策を見直し①利用できる管理策②例外措置が必要な管理策③現場に選択させる管理策を明確にする。例外措置となったものは全社ベース、地域ベースで検討する。手法として以下の2つを示す。

(1)制御システムのOTのセキュリティ例外対象の明確化(ISO/IEC27002より)
以下を目的とし,OTの例外対象の明確化を鉄道システムを例に検証した
①ISMSから外れる管理策はどこか、リスクがあるか管理を容易化する
②例外対象を明確にし、組織統制を行い基本方針、対策基準を作成する
③例外部分についての理由、代替管理策を明確にしておく
④情報システムとの連携、接続を見据えISMS基準にリスク評価を実施



この例では、左側にISO/IEC27002の管理策を記述した「基本管理策」、中央側に「例外可否」として、運行管理の演算処理を行う中央サーバをシステムA、現場設備機器をシステムBとして分け[●(例外措置可)][○(一部例外措置可)][ー(例外措不可)]と示す。右側に「例外理由・条件・代替策」を記載した。これにより、鉄道システムを当てはめ検証したところ、管理策114個中82個の管理策はそのまま使え、システムAの例外対象は14個、システムBの例外対象31個で有ることがわかった
さらに、管理策全体を本社で管理するもの、地域で管理するもの、現場で管理するものに分けられることがわかった。この結果、提案手法が実際に活用できることがわかった。

(2)現場運用セキュリティフレームワークの提供(鉄道会社組織例)
上記のフレームワークを鉄道会社組織を例に運用フローを示す。
経営層・本社機能部門から運用部門が対策基準、実施手順を作るためのフレームワーク(上記の例外対象)を規定、提供するその後、運用部門で例外措置を再検討し、現場に合わせた対策基準及び実施手順を作成する。その後、本社機能部門で例外措置を最終承認する。



4. まとめ

(1)制御システムの特徴・変化・課題を明確にした
(2) ISMSを基準とした管理策から例外対象を明確化・運用する手法を提案した。今後情報システムへの連携やリスク管理において脆弱箇所を予め把握することが可能
(3) 鉄道システムを一例にして、フレームワークを実際に適用し実際に使えることを示した。今後のリスク管理、評価に役立て、組織で運用できることを示した